Current Threats of Wireless Networks

Mardiana Mohamad Noor and Wan Haslina Hassan

Communication System and Network (iKohza) Research Group,
Malaysia Japan International Institute of Technology (MJIIT),
Universiti Teknologi Malaysia.

mardianamnoor@yahoo.com, wanhaslina@ic.utm.my

ABSTRACT
This paper discusses current threats in wireless networks. Advancement and countermeasures for each threat such as sniffing, Man In the Middle Attack (MITM), Rogue Access Points (RAP), Denial Of Services (DoS) and social engineering are discussed in this paper. Some practical suggestions for service providers and users to mitigate the risks to the threats are also presented.

KEYWORDS
Current threats in WiFi, risks mitigation in WiFi, network scanning, password cracking, MITM, jamming attack, Rogue Access Points, countermeasures of wireless threats

1 INTRODUCTION

Wireless networks are susceptible and exposed to attack because of its borderless nature. Threat which is any action that causes security breach is very significant in wireless network. For example packet sniffing can be done passively because of the hub-based configuration of the access points in wireless networks. Despite the ease of deployment of such activity, it initiates more dangerous attacks such as Man In The Middle (MITM) attack. MITM attacks such as session hijacking and MAC spoofing are some of the critical threats for wireless networks. In reality, hacking tools are largely available in the market and online. These tools are usually meant to be used by penetration testers and for educational purposes are being misused and abused by underground hackers. Therefore, the sophistication and frequency of attacks have increased; by just using ready to use tools. On the other hand, the flexibility and ubiquity of mobile devices such as smartphones, tablets, phablets and laptops are the main reason of the popularity of hotspots which are exposed of the rogue access points.

From the data gathered by Malaysian Communication and Multimedia Commission (MCMC) [1] until the second quarter of 2012, 1.2 million of registered hotspots were recorded. For the purpose of comparison, in 2011, only 0.4 million hotspots were registered. These statistics show that the number of hotspots subscription in 2012 is rather large. In other word, in Malaysia particularly, internet users are moving towards wireless connectivity. This scenario will definitely raising the bar of security measures that should be taken especially in curbing intrusion into wireless networks.

Cases of misuse, incidents and threats of internet have been reported in Malaysia since 1997 to Malaysian Computer Emergency Response Team (MyCERT) [2]. Numbers of cases reported keep increasing tremendously year by year which confirm the upward trend of internet threats. The statistic from the report shows that the pattern of attacks changes from time to time which basically follows the development of the internet. From 1997 until 2003 most of the incidents reported were due to spam and virus cases, but from 2004 until 2011 there is tremendous incline in the attempt to intrude and intrusion of the network attack. In 2003 only 60 cases due to intrusion were reported, but in 2004, 368 cases were reported. In the same report, the inclination is very obvious

from 2007 until 2011 when attacks due to intrusion increase sharply by 861%.

In this paper we present current and persistent threats to wireless networks and accompanied by some active researches from academia regarding the advancement and some counter measures to the threats.

The second section of the paper discusses some current threats in wireless networks and researches of developments and countermeasures to the attacks. The third part discusses security risks to the wireless network due to the advancement of cloud computing, and the fourth section presented some new hacking tools available on the market. The last part of this paper presented some analysis and some recommended counter measures to threats in wireless networks.

2 THREATS OF WIRELESS NETWORKS

2.1 Network Scanning and Password Cracking

Network scanning is a process when hackers use tools to scan the network. The objectives of this activity are to:

a) find the vulnerabilities and security level of the network
b) determine signal strength
c) determine the accessibility of the target network
d) map the target network

After scanning the network, the attacker might proceed to get into the network. Despite of the known weaknesses of WEP, it is still in use because of the several reasons which involves some issues of installation, interoperability, convenience and flexibility.

In the following researches are the evidences of vast availability of network scanning tools and some of them are open sources. In [3] and [4] war driving activities were carried out by using different tools and platform. In [3] it has been found that Cain and Able outperformed Netstumbler and Kismet in terms of functions because it possess ARP poison, VoIP logger, password crackers and built in WiFi scanner in the expense of volume of access points detected. In [4] wardriving activity using Windows and Mac operating systems were conducted concurrently and comparison and analysis of the best scanning tools using both platforms were presented. This research concluded that inSSIDer is the best tool (shows vendor of the access point and indicate signal strength graphically) using Windows operating system and KisMAC is the best tool for Mac (detects WiFi silently, channel tuning capability and detects wireless clients connected to the access point).

In [4], a war driving was conducted in several neighbourhoods in Dubai, UAE in order to investigate the current WiFi security issues. A laptop running MAC OS X and a WiFi scanning tool and a car were used in the war driving. From the war driving in four different neighbourhoods a total number of 1,228 WiFi networks were found. Four categories of WiFi networks have been found which are:

a) Open Network – WiFi networks that did not implement any protection - 35%
b) WiFi implementing Wired Equivalence Privacy (WEP) - 26%
c) WiFi implementing WiFi Protected Access (WPA) - 30%
d) WiFi implementing WiFi Protected Access 2 - 9%

From the war driving experience more than 50% of the residents have no security or implementing weak security protocol.

Researches to attempt cracking WEP and WPA/2 were done in [5-8]. Series of attempts by Fluhrer, Mantin and Shamir (also known as FMS), and later in 2004 a person under pseudoname KoreK made a second attempt and succeeded. Tews, Weinmenn and Pyshkin (known as PTW) launched new generation attack in 2007 followed by a Chopchop attack. Based on these successful attempts, cracking tools were developed. In WEP mode even though the length of the passphrase is increased or complicated, only 30 minutes were taken to break the code. Nevertheless, users which are using WEP because of the convenience of setting and interoperability, are advised to set proper passphrase which will take longer time to break and will create noise in the network.

Even though WPA/WPA2 is said to be robust, it is still protected by a passphrase which can be cracked by using “Dictionary Attack”. In [8], a new proposed space-time trade off solution is used where the Pair Master Keys (PMK) are pre calculated for each passphrase in the library and

store them into another library called Hash Library. This research also suggested employing cloud computing to generate possible passphrase and to take GPU parallel computing into consideration to effectively calculate PMK and proofread the Hash Library.

This section concludes that with the matured amount of wardriving and password cracking activities had developed the advanced and powerful tools for network scanning and password cracking.

2.2 Man In the Middle Attack (MITM) and Packet Sniffing

MITM attack is to position the attacker between two hosts in order to hijack connection and injecting traffic. In wireless networks, MITM can occur as jamming by consistently transmitting signals to the existing wireless access points while providing clear signal from another fake access points. Another MITM attack is by using a spoofed de-association or de-authentication frames to hijack the connection between legitimate AP and the users [9]. Wireless networks are more susceptible to the kind of attacks because it causes less disturbances if the attacker poses as one of the client hosts in order to access the network and launch attack to a single host.

Packet sniffing is another significant threat to wireless networks by using packet sniffer such as Wireshark, Network Miner or Cain and Able. During this attack attacker usually sniff the content of packets and access unencrypted usernames and passwords.

In [10], the author has listed out the security risks from this activity such as eavesdropping, breaching the credentials, session hijacking by stealing the victim's session website's cookie and revealing one's internet activities. By using tools such as Wireshark, Ethercap or NetworkMiner, sniffing activities can be done by anybody by little practice. The author of [10] also stated that most of the Internet runs in the plaintext, making it readable by packet sniffers, but if the conversation is run through encrypted connection such as site using SSL encryption, data is less vulnerable. It is also revealed that session hijacking is also possible in sniffing activity by stealing victim's session cookie for a particular website, especially when the websites do not encrypt their traffic to the end user.

Packet sniffing can be a handful task to perform in large networks because of incapability of the tools to sniff large amount of packets. A sophisticated form of packet sniffing is presented in [11], where a passive monitoring system for complex wireless network is designed. This research is to design a robust framework to monitor real time network passively on a large scale WiFi network. In [11], volume of data gathered from sniffing activities was reduced, so the system was capable to listen to the traffic in the larger radius.

2.3 Rogue Access Points (RAP)

The purpose of RAP is to hijack the connection of legitimate users is in order to sniff the activities or to steal confidential credentials of the users and later launch further attacks. With the availability and competitive price of access points (AP) in the market, anyone can set a fake access point especially in free WiFi hotspots. Moreover, nowadays most of the laptops can function as a soft AP. According to EC Council [12], there are at least four available APs nowadays, which are:

a) Compact and pocket sized RAP device plugged into an Ethernet port of corporate network
b) Software-based RAP running on a corporate Windows machines
c) RAPs connected to corporate network over a WiFi link
d) USB-based RAP access point device plugged into a corporate machine

RAPs are usually placed behind a firewall to avoid network scanner.

Counter measures to RAP is an active area of research which concentrate at two end points which are client side and administrator side solutions. The advantage of having RAP solution in the network administrator side is users are warned about the safety of the connection automatically every time they are using one particular wireless network.

In [13] a full automated concept which is to detect and eliminate RAP at the network administrator side by using mobile agents, namely

master and slave agents was introduced. A master agent is generated on the server and then generated slave agents according to the numbers of APs. If any new AP exists slave agents will be cloned. When a client find a new AP, information of the packet will be created and the clone slave agent will bring the information to the slave agent and the information will be sent to the master agent to be verified. Master agent will match the information with the repository and if it is not matched then the AP will be eliminated. This method is claimed to be easy to implement, reliable and cost effective. This method is seen as a robust method to detect and block RAPs.

In [14], another RAP counter measure at network administration side solution was proposed which is a centralized passive Indirect Rogue Access Points Detection System (RAPiD). RAPiD is to discover and verify RAP by collecting data at routers or gateways and send the packets to the network wireless host engine which will be used to track each unique local network host and determine whether a host is using the wireless network or not. However, the results of RAPiD dependent on wireless host discoveries and authorization verification.

In [15] developed an intrusion detection scheme based on social network and biomimetic approach. This first part of this research is to propose "sneeze" algorithm which is analogous to human immune system. In this algorithm it is assume that all APs are virtually connected to each other and aware of the presence of each AP. Each AP periodically acts as a node and monitors the presence of APs by tracking the Basic Service Set Identifier (BSSID). If any RAP is placed within the subnet, it will detect its presence and availability of the beacon signal and its BSSID. Then it will check the AP with the list of APs it has in its list. If the AP is not in the list, it changes its access key and alerts the network administrator to physically remove the RAP from the network. This discovery has reduced the work of network administrator from constantly monitoring the network. Once the RAP was found by the "sneeze" algorithm, network administrator will physically remove the RAP.

Consistent monitoring and the list of known legitimate APs are the criteria needed in order to implement network administrator side solution. Another obvious weakness of this solution is because of the scale of the network is usually immense, accuracy in the executed algorithm might be jeopardized and users might get false alarm of RAP or wrong information about the illegitimate APs.

In [16], an end user solution has been proposed in order to detect RAPs especially in public hotspots. In this proposed work, a flexible and practical solution is suggested, especially for mobile users or travellers to protect their credentials where the security monitoring is not reliable. The technique proposed was based on the knowledge that in the existence of RAP, the client has to communicate with a remote server through an evil twin AP and a normal AP. In this case, compared to the normal scenario, the twin evil case has one more wireless hop. To distinguish these two cases (one and two wireless hops), Inter-packet Arrival Time (IAT) statistic, which is a time interval between two consecutive data packets sent from the same devices has been adopted. A prototype system called Evil Twin Sniffer (ET Sniffer) which has been evaluated in real wireless network including 802.11b/g was introduced by using two novel algorithms which are Trained Mean Matching (TMM) and Hop Differentiating Techniques (HDT). The analysis from the experimental set up yields ET Sniffer can detect illegitimate APs quickly with high accuracy and resilient to changes in wireless environment.

In [17], Somayeh et al proposed a novel method for RAP detection on the client-side which is able to detect both MITM attack and evil twin attack. This is a client side detection method where clients' mobile will be warned on the safety of the network by indicating different colours of lights namely green (safe), yellow (RAP is present) and red (MITM attack). In this research, a method to decide whether the network is exposed to RAP, tricked by RAP or is it a safe network is designed by comparing SSIDs, MAC and IP address of the public APs. Green light will be indicated if the network is safe to connect to, yellow indicates the existence of RAP and red light is the sign to warn the users of the MITM hazard in the network.

These are solutions which are suitable for mobile users whom always use their devices in places prone to RAP such as airports and hotels. The disadvantages of client side solution are users have to implement and be familiar of the introduced algorithm and simple WiFi enabled devices might not support the proposed algorithm.

2.4 Denial of Service

One of the weaknesses of wireless network is the restricted usage of bandwidth. This situation is giving great advantage to hackers to launch Denial of Service attack by replaying packets in order to generate noise or by sending de-authenticate packets to the legitimate users in the subnet. In fact, according to Belly Rachdianto [18], this is the technique used by a large group of hackers, 'Anonymous' to bring down governments web servers in the recent attacks.

Practically, jamming attack is a popular attack in military battlefield usually by exploiting the weaknesses of Wireless Sensor Network (WSN) which have limited power resources. Jamming attack can be launched either from outside or inside the network by using jamming devices to block the wireless medium and prevent wireless devices from communicating with each other in order to degrade the performance or to paralyze the network. Some researches presented herewith are advancements in jamming attack which could be launched from internal and external of the network.

Liu et al. in [19] have proposed mobile jamming attack to Wireless Sensor Networks (WSNs). In this attack, the mobile jammers are placed randomly in the network, listen to the network traffics and detect the cluster head based on received signal strength (RSS). According to [19], the attack to the cluster head node is an effective method because if the communication between this node and sink node is interrupted the base station may not get any information. The results show that mobile jammers has longer lifetime corrupted and less energy is needed for mobile jammers to bring down a WSN.

In selective jamming/ dropping as proposed in [20], the targeted channel which was defined by separate frequency band, time slot or Pseudo Noise (PN) code will be under attack or the attacker will select data of high importance by observing specific packet identifiers. Due to the nature of selective jamming, this type of attack is not easy to detect as aggregate behavioural metrics are unable detect attacks of selective nature, when only a small fraction of packets were under attacks.

Random Packet Distribution (RPD) is a type of external jamming attack when the specified attack model is well-protected with various security measures [21]. RPD jammer is put at the area of APs in a Wireless Mesh Network (WMN). At this point, the jammer will destroy the packets by transmitting a short period of noise signal when packets transmission is detected. According to [21], any kind of encryption and authentication may not mitigate the risk of such attack because the attacker does not need to participate in the network.

In this investigation, the analysis of damages caused by this attack was conducted using Qualnet Network Simulator. Performance metric such as goodput, delay, jitter and Mean Opinion Score (MOS) were analysed. The simulation also showed that real time applications such as (Voice over Internet Protocol) VoIP will be adversely affected. MOS score shows that at 5% attack rate can affect the voice quality. Based on the analysis of TCP's throughput in [21], packet lost rate at 20% can bring down a network, which is equivalent to 40% RPD attack rate.

In another research, Distributed Jammer Network (DJN), utilizes the advantages of nano-technology, where the jammers are not visible in the naked eyes is proposed by Hong et al [22]. These low powered jammers are claimed to have less self-interference. DJN has few distinguish advantages which are:

a) because DJN is composed of a large number of devices of ample redundancy, it is claimed to be robust

b) DJN emits low power, which is advantageous because of health

c) It is hard to detect due to its very small size

To measure the impact of DJN, a scenario is simulated in QualNet and the result revealed that DJN can cause phase transition even though the power is held constant.

From these researches it has been proven that jamming attacks are potentially energy efficient, silent and hard to trace and robust means of attacks.

2.5 Social Engineering

Social engineering is the art of utilizing human behaviour to breach security without the victim realizing that they have been manipulated. Social Engineering can be categorized into two categories which are technology based deception and human based deception [23].

Study in [23] revealed that here are several behaviours that are vulnerable to this attacks which are trust, carelessness, curiosity and ignorance. Social engineering attacks mostly will affect big companies and organization where the workers and people inside the organizations are the victims of the threats. The effects of this attack can be in monetary form, where a company can suffer billions of loss due to data leakage and distrust from the existing customers and compromised reputation.

The only way to mitigate security risks from social engineering is to educate the entities in any corporation in order to create awareness to the social engineering threats.

2.6 Threats in Bluetooth Technology

Saroj *et al* [24], has discussed threats in piconet and medium range wireless networks such as Bluetooth, RFID and Wireless Sensor Network (WSN).

Bluetooth technology which enabling file transfer and other data communication between devices such as printer, PDA and smartphones are vulnerable to threats which are classified as in ABOTT (A Bluetooth Threat Taxonomy) which is listed below.

a) Surveillance – Bluprinting, bluefish, sdp tool
b) Range Extension – BlueSnipping, bluetone
c) Obfuscation- Spooftooth
d) Fuzzer – BluePass, BlueSmack
e) Sniffing – BlueSniff, Wireshark
f) Denial of Service – Signal Jamming, Battery exhaustion
g) Malware – BlueBag, Caribe
h) Unauthorized direct data access – Bloover, BluBug
i) Man in the middle – BlueSpoof

2.7 Threats in RFID

RFIDs are used as smart tags which are widely deployed and it also exposed to many kind of threats; which is similar to attacks in WiFi. Some of the common attacks are sniffing, tracking, spoofing, tracking, replaying and Denial of Service attack. The most critical attack in RFID is replay attacks which enable the attacker to intercept and retransmit RFID queries.

3.0 Cloud Computing : The Security Risks to the Wireless Communication

Services offered by cloud are data storage, software, platform and infrastructure [25]. According to Tim Pierson, a professional PenTester and consultant in Hacker Halted Conference in Kuala Lumpur, internet users have been using cloud especially as storage mechanism for years for example Gmail, Amazon and YAHOO [26].

One of the latest developments of cloud computing is making one's WiFi accessible from anywhere. This is a practical and flexible solution as it comes with many applications developed by third party. In June 2012, Cisco has launched its 'smart Wi Fi' product which is Cisco Connect Cloud [27]. On the other hand, this development raises other privacy and security issues since there is no guarantee that the cloud service, provider will not share users' WiFi configuration and other confidential credentials.

Cloud computing also might solve some problems of the retailers such as distributed natures, scalability, security monitoring and reduces the cost of WiFi deployment [28]. Since cloud is shared between tenants, this might lead to data intrusion and motivate hacking Wi Fi through cloud. One example of cloud abuse has been reported in 2011, where some powerful software leased from Amazon has been used to hack WiFi WPA through brute force attack [29]. Not to mention some security issues in the cloud itself which are very appealing to the hackers to launch attack. If hackers can attack the cloud, the network associated with it is jeopardized.

4.0 Hacking Tools

The attacks in wireless network are aided by tools and some of the tools have been used in attacks explained in section two. Furthermore, the devices proliferation for wireless hacking tools online which require minimal technical skills and easy to execute such as Raspberry Pwn, Nokia N900 PwnPhone, and Wi Fi Hot Spot Honeypot trigger more hacktivism. In the recent Hacker Halted Conference on 19 November 2012 in Kuala Lumpur, Wayne M Burke, the CEO of Sequrit [30], has presented some of the mobile hacking tools as said above and found that those tools are being sold from as low as USD 99.99. These tools are merely for the security professionals and for the educational purposes, but also have great potential to be misused, abused and exploited by hackers. The vast development of these mobile devices which have permanent connectivity to the internet can be used to spy, drop malicious code (malware), monitoring person by GPS, redirected the email and read messages.

4.1 Raspberry PwnPi

This tool is a fully-featured security penetration and auditing platform [31]. It has comprehensive hacking tools which will lure the hacker to attack wireless medium which include information gathering, network mapping, penetration and vulnerability identification. It also releases free community edition, which is definitely an excitement to all the hackers.

4.2 Nokia N900 PwnPhone

Nokia N900 is mobile-phone-based-pentesting platform which includes Aircrack-NG, Metasploit, Kismet and also featuring one–click evil AP, WEP Cracker and a packet capture. This comprehensive device is available in the market at the price of USD 995.00.

4.3 WiFi Hot-Spot Honeypot

The WiFi Pineapple Mark IV is one of the favourite multi-functional penetration testing platform since 2008 [32]. Especially used to launch the man-in-the-middle attack, which is also enabling it to observe the connected client, perform site surveys, customize attacks and capture data in a few clicks. It also functions as a mobile broadband, Android tether, WiFi relay and provide internet connectivity to PC. Despite of its comprehensive capability and functions, this device is available at a very affordable cost, which is USD 99.99.

4.4 Open Source Intelligent (OSINT)

One of the famous hacker namely 'The Jester' has revealed his favorite hacking tools as OSINT. The tools such as Maltego, Creepy, Spokeo, CaseFile and FoxOne Scanner (to name a few) can be downloaded easily and exploited by malicious hackers. In fact, all of the downloadable programs even come with step-by-step tutorials and provide details information of the said programs.

4.5 Mobile Vulnerabilities

Recently, it also has been reported that there is a flaw in wireless chipset design provided by a wireless semiconductor manufacturer, Broadcom Corporation in which will make the affected smartphones prone to DoS attack [33]. Broadcom BCM4325 and BCM4329 wireless chipsets have been reported to contain out-of-bound read error condition that might be exploited to produce a denial of service condition. Upon the writing of this survey paper among the smartphones which have been planted with these chipsets are Apple iPhones, Motorola, Samsung, HTC, LG and Sony Ericsson.

5. FINDINGS AND ANALYSIS

Hackers' intent to target a wireless network is to exploit the network users' privacy in a MITM attack, to perform privilege escalation and to use hotspot as a platform to attack a nearby target and remain untraceable. The main reasons for hacking activities are the opportunities to exploit vulnerabilities and the ease to execute attacks. The seamless boundary of wireless network is making the networks easy to penetrate while the availability of free public WiFi is making these malicious activities easy to launch and possibly done by novice hackers. One interesting fact learnt from reviewing the research papers is the sophistication of the attacks is increasing while the skill needed is very minimal. This is probably due to the misuse of the

penetration testing tools which are affordable and easy to use and carry and the vast availability of hacking software on the internet.

RAPs are usually found in public hotspots. With the availability and competitive price of physical access points and with a little practice and training, anyone could install a RAP to any public hot spot. Furthermore, RAP is almost invisible especially when the attacker uses his own laptop as a soft access point. This threat is actually leads to another dangerous attack which is Man In The Middle (MITM). In wireless network MITM is dangerous because it is a passive and silent attack which listens and sniffs users' conversation and most probably will intercept and modify the packets being relayed. MITM is almost impossible to prevent as long as the attacker find a "hole" to access the network, legally or not. MITM can lead to another disastrous attack, for example session hijacking.

People are always the weakest link in security. The threats posed by social engineering are almost destructive as other technical threats. The art of deception is the most useful skill in social engineering, while insiders' ignorance and negligence always open the door for the opportunist attackers to cause security breaches.

On the other hand, a lot of researches on improvisation of the attacks and counter measures against the attacks have been carried out. For example, Denial of Service attacks especially jamming attacks have gone through many phases of advancement in terms of capability and invisibility, while countermeasures techniques to evade RAPs are also on the rise.

Everybody is exposed to threats in wireless network as no network is fully guaranteed as secured. Hence, network administrators and users must be more serious in curbing security issues in wireless networks and apply countermeasures to lessen the risks of security issues. Here are some practical recommendations for countermeasures to the threats in wireless networks from service providers' side:

5.1 Change the default Service Set Identifier (SSID).

Having known the value for the SSID for the router and access point is the initial step to break through a wireless network. Usually, when an attacker sees a SSID with a default value, he will assume that the network is poorly configured. Sometimes, the default SSID is also used as the password to the network.

5.2 Turn On the Encryption

Be it WEP or WPA/2, encryption must be turned on. It is much better than leaving the network as the open network. No network is guaranteed secure, but at least precautions can be taken so that the attack is less likely to occur and more difficult to launch. Stronger algorithm such as CCMP is recommended for the encryption or even better to invest using WPA the Enterprise mode. Network administrators are also advised to set stronger password to avoid novice hackers from cracking it. It also recommended changing the password regularly.

5.3 Disable SSID Broadcast

By broadcasting the SSID into the air, it tells the existence of the network without any effort. It is like calling hackers to break into the network. Broadcasting SSID is less likely necessary in the home network.

5.4 Place the Access Point Securely

In order to control access to our WiFi network, the access point must be placed appropriately so that the signal in the desirable radius.

5.5 Policy Enforcement

By having clear and understandable policy or agreement of prohibited actions in wireless network such as packet sniffing or placing any device which can act as a RAP might help to reduce malicious activities in wireless network. As to handle threats that might occur because of social engineering, a written agreement of policy between employer and employers must be taken place from the first day of work. Employers might have been given certain unique password to login into company's WiFi network and repeatedly reminding them not to share the password and other sensitive credentials to others.

Precautions must also be taken when the users are using wireless network outside of their homes or offices, such as hot spots to safeguard confidential credentials from any attackers. Here are some advices:

5.6 Disable the WiFi adapter

This is important to prevent auto connection from the malicious access point in the network. It is also important to always monitor the access point that will connect to the PC by configuring the setting in the PC.

5.7 Secure Your Network

Users are advised to use Virtual Private Network especially to prevent Man In The Middle attack. Activating firewall is also another method to secure the network.

5.8 Secure Your Confidentialities

By disabling file sharing feature will mitigate the risk of the threats. By encrypting and setting privacy to important folders are other precautions when using public WiFi.

5.9 Prevent Auto Connection to Open WiFi

Some computers will automatically connect to the open wireless network without giving you any notification. It is also advised not to control the wireless network remotely and always disable the network when not in use in a long period of time.

6 CONCLUSIONS

As presented in this paper, wireless networks are susceptible to attacks and prone to many types of threats. This is due to its seamless nature and its popularity. Users in public hotspots are claimed to be more exposed to such threats because of the ease to deploy MITM by sniffing techniques and planting RAPs. The vast availability of the hacking tools and devices opens up wide path for hacktivism, while the advancement of cloud computing making Wi Fi more vulnerable to threats. The security of cloud computing as well must be managed very well to avoid leakage and breach of information.

.

7 REFERENCES

1. Number of registered hotspots in Malaysia Q2, Pocket Book of Statistics Q2 (SKMM), 2012. www.skmm.gov.my.
2. Reported Internet Incidents from 1997-2012 (MyCERT), www.mycert.org.my.
3. Reddy, S.V., Rijutha, K., Ramani, K.S., Ali, S.M. : Wireless Hacking – A WiFi Hack By Cracking WEP. In: Proc 2010 Second International Conference on Education Technology and Computer (ICETC) 2010.
4. Said, H., Guimaraes, M., Mutawa, N.A, Awadhi, I.: Forensics and War Driving on Unsecured Wireless Network. In: Proc 2011 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi (2011).
5. Begh, G.R, Mir, A.H.: Quantification of the Effect of Security on Performance in Wireless LANs. In: Proc. 2009 Third International Conference on Emerging Security Information, Systems and Technologies (2009).
6. Mavridis, I.P., Androulakis, A.I, Halkias, A.B., Mylonas, P.: Real-life Paradigm of Wireless Network Security Attacks. In: Proc. 2011 Panhellenic Conference on Informatics (2011).
7. Beck, M., Tews, E.: Practical Attacks Against WEP and WPA. In: Proc. 2009 Second ACM Conference on Wireless network Security (Wisec) 2009..
8. Yin, D., Cui, K.: A Research into The Latent Danger of WLAN. In: Proc.2011 The 6th International Conference on Computer Science and Education ICCSE, Singapore (2011).
9. Andrew, A. Vladimirov, Gavrilenko, K.V, Mikhailovsky A.A.: WI-FOO: The Secrets of Wireless Hacking: Breaking Through. Pp—155-173 Pearson Education (2004).
10. Hannah, A.: Packet Sniffing Basics. http://delivery.acm.org
11. Benmoshe, B., Berliner, E., Dvir A., Gorodisher, A.: A Joint Framework of Passive Monitoring System for Complex Wireless Networks. In: Proc. 2011 First International IEEE Workshop on Emerging Densely Connected Networks (EDCN) 2011.
12. EC Council (2012). Certified Ethical Hacker: Hacking Wireless Networks, Module 15. pg 91-93.
13. Sriram, V.S.S, Sahoo, G., Agawal, K.K.: Detecting and Eliminating Rouge Access Points in IEEE-802.11 WLAN – A Multi-Agent Sourcing Agent Methodology. Birla Institute of Technology, India (2010).
14. Qu, G., Nefcy, M.M.: RAPiD - An Indirect Rogue Access Point Detection System. Oakland University, Michigan USA (2010).
15. Sampangi, R.V, Dey, S., Viswanath, V.N.: The Sneeze Algorithm: A Social Network and Biomimetic Approach for intrusion Detection in

Wireless Networks. University of Mysore, Mysore India (2010).
16. Song,, Y., Yang C., Gu, G.: Who is Peeping at Your Password at Starbucks? – To Catch an Evil Twin Access Point. In: Proc. 2010 IEEE/ IFIP International Conference on Dependable Systems and Networks (DSN).
17. Nikbakhsh, S., Zamani, M., Abdul Manaf, A., Janbeglou, M.: A Novel Approach for Rogue Access Point Detection on the Client Side. In: Proc. 2012 26th International Conference on Advanced Information Networking and Application Workshop.
18. Rachdianto, B.: Threats in Wireless Networks: In Tutorial Ethical Certified Hacker, EC Council (2012) pp 1--39
19. Zhiping, L., Hui, L.:Mobile Jamming Attack in Clustering Wireless Sensor Network. In: Proc. 2010 International Conference on Computer Application and System Modelling (ICCASM) 2010.
20. Lazos, L., Krunz, M.: Selective Jamming/ Dropping Insider Attack in Wireless Mesh Network (WMN). University of Arizona 2011.
21. Zhou, B., Marshal, A., Zhou, W., Yang, K.A.: Random Packet Destruction DoS Attack for Wireless Networks. In: Proc. 2008 ICC.
22. Huang, H., Ahmed, N., Karthik, P.: On a New Type of Denial of Service Attack in Wireless Networks - The Distributed Jammer Network. In: 2011 Proc. IEEE Transactions On Wireless Communications.
23. Gulati, R :The Threat of Social Engineering and Your Defence Against It. In SANS Institute Info Sec Reading Room 2003.
24. Panigrahy, S.K, Jena, S.K, Turuk, A.K.: Security in Bluetooth, RFID and Wireless Sensor Network. In: Proc. 2011 ICCCS'11, India (2011).
25. Yu, H., Powel, N., Stembridge, D., Yuan, X.: Cloud Computing and Security Challenges. In: Proc. 2012 50th Annual Southeast Regional Conference (2012).
26. Pierson, T.: Cloud Computing- APAC Hacker Halted Module: In Hacker Halted Conference 2012.
27. Cisco "SmartWiFi". http://newsroom.cisco.com/press
28. Why retailers embrace cloud WiFi access http://blog.airtightnetworks.com/why
29. Amazon Cloud Could Help Hack WiFi Networks http://www.reuters.com/article/2011/01/07/us-amazon-hacking-idUSTRE70641M20110107
30. Wayne M Burke in Hacker Halted Conference November 19, 2012, Kuala Lumpur.
31. Advance Persistent Pentesting http://pwnieexpress.com/
32. Hotspot Honeypot Pentesting Platform http://hakshop.myshopify.com/collections/gadgets/products/wifi-pineapple
33. Vulnerabilities in Mobile Devices http://thehackernews.com